PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 12/56, 29/06

A1

(11) International Publication Number: **WO 00/56023**

(43) International Publication Date: 21 September 2000 (21.09.00)

(21) International Application Number: PCT/SE00/00503

(22) International Filing Date: 13 March 2000 (13.03.00)

(30) Priority Data:
09/267,060 12 March 1999 (12.03.99) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) [SE/SE]; S–126 25 Stockholm (SE).

(72) Inventor: ERIKSSON, Örjan; Gåsmossen 37, S–436 39 Askim (SE).

(74) Agent: NORIN, Klas; Ericsson Radio Systems AB, Common Patent Department, S–164 80 Stockholm (SE).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

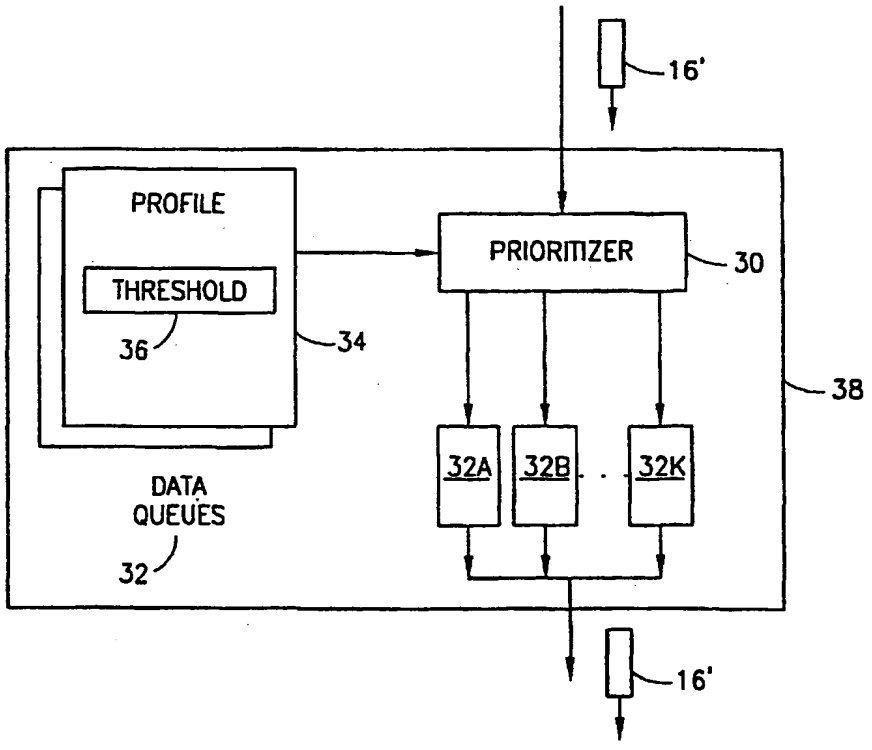
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHODS AND ARRANGEMENTS FOR POLICING AND FORWARDING DATA IN A DATA COMMUNICATIONS SYSTEM

(57) Abstract

Improved policing and forwarding methods and arrangements are provided for use in data communication systems (10) and networks (14, 26) that transport different classes of packetized data, as differentiated, for example, by a priority label (40) associated with a desired quality of service (QoS). A policing (38) module monitors traffic flow for selected classes of packetized data (16) and if corresponding threshold values (36) are reached, then the packetized (16) data is handled according to a lower priority scheme. In this manner, higher priority packetized data is not simply dropped or otherwise ignored when the higher priority forwarding scheme is saturated or overflowing. Instead, the higher priority packetized data is handled as a lower priority packetized data, thereby significantly increasing the QoS provided and also providing additional resource control to the service provider.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHODS AND ARRANGEMENTS FOR POLICING AND FORWARDING DATA IN A DATA COMMUNICATIONS SYSTEM

Technical Field of the Invention

The present invention relates to data communications and, more particularly, to improved methods and arrangements for policing and forwarding data carried within a data communications device, network, or system.

Background

The two-way transmission of audio over an Internet Protocol (IP) configured network is often referred to voice over IP (VoIP). With VoIP, telephone conversations can be conducted between two or more parties connected to the Internet, intranets, and/or private local area networks (LANs) and wide area networks (WANs) that use the transmission control protocol/internet protocol (TCP/IP) routable communications protocol suite.

Certain intranets and other private networks can be configured to provide VoIP services that are comparable in quality of service (QoS) to traditional public switched telephone networks (PSTNs). Since VoIP is a packet-switched technology, VoIP packets or datagrams can be routed or otherwise handled in a way that maximizes the use of shared communication resources and circuits. For this reason and others, traditional telephone service providers (which typically provide a dedicated circuit connection for each call), have begun moving toward VoIP and other similar packetized communication technologies.

Unfortunately, the quality of service (QoS) provided by VoIP connections over many large networks, and especially, for example, the Internet, can vary considerably. The varying QoS for VoIP connections is typically a function of the level of traffic on the network, compared to the available sources.

To provide realtime communications, such as in the case of VoIP connections, the datagrams containing audio and/or video information are inherently time-sensitive. As such, the datagrams need to arrive at the receiving node in a timely order. Thus,

for example, the information contained within late arriving or otherwise delayed datagrams is not provided to or used by the receiving node's application. It is this "dropped" or delayed information that tends to significantly reduce the QoS provided.

A conventional TCP/IP protocol suite includes several protocols configured to increase the QoS for selected datagrams. For example, a user datagram protocol (UDP) is provided for use in place of TCP. UDP can be used for realtime audio and video traffic where lost datagrams are simply ignored, because there is no time to retransmit (as typically required by TCP). Further, a realtime transport protocol (RTP) is provided for use with audio and video transmissions. RTP provides additional time stamping and synchronization information for use in reassembly of audio and/or video information at the receiving node. Other protocols are also known, such as, for example, a realtime streaming protocol (RTSP) is used to transmit audio and/or video over IP, and a reservation protocol (RSVP) is used by routing nodes within the network to reserve bandwidth for realtime transmission of audio and video

Using these various protocols and associated techniques, there are basically two methods currently available for achieving an expected QoS in an IP data communications network. The first method is a connection oriented method in which new sessions or applications, which require more than the typical "best effort" QoS (i.e., no guaranteed QoS), have to reserve capacity or bandwidth from the source node to the receiving or destination node. Thus, for example, RSVP can be used to reserve bandwidth over a network. Reserving bandwidth over the network, however, tends to decrease the efficiency of the network.

The second method is a connectionless oriented method, wherein the datagrams are associated with a desired priority setting or label and the various routing nodes within the network are configured to route datagrams in a manner relating each datagram's priority label. Thus, for example, certain differentiated services are being proposed by the Internet Engineering Task Force (IETF) in which a priority label is included in the type of service (ToS) byte within Internet Protocol Version 4 (Ipv4).

This connectionless oriented method can be implemented in a variety of ways. For example, International Patent Application Number WO 97/36405, entitled "Prioritization of Data to be Transmitted in a Router," discloses that radio transmitted

packets can be selectively routed within a radio accessed network using data queuing techniques associated with the desired QoS (e.g., priority label) or a subscriber's identity. Such queuing techniques cause higher priority datagrams be sent before lower priority datagrams (e.g., best effort datagrams). This tends to increase the QoS for the higher priority datagrams, such as, for example, datagrams containing audio and/or video information. Unfortunately, for such systems, there remains a potential for dropped audio and voice information should the various higher priority data queues overflow.

Consequently, there is a need for improved data transmission methods and arrangements that differentiate between different priority data, reduce dropped data, and provide a reliable QoS for selected priority data transmissions.

SUMMARY OF THE INVENTION

The present invention provides improved data transmission methods and arrangements that differentiate between different classes and levels of priority data and handle the different classes of data in a way that reduces the chance of dropping higher priority data, thereby providing a more reliable quality of service (QoS) for selected priority data transmissions.

In accordance with certain aspects of the present invention, data packets are marked with a priority identifier and handled accordingly. If, however, a forwarding node cannot handle any additional higher priority data, for example, because of high traffic volumes and overflowing data queues, then the higher priority data packet is handled as a lower priority data packet. This allows the higher priority data packet to possibly be forwarded rather than simply dropped. In certain situations, this policing scheme significantly increases the QoS. Additionally, the service provider is provided increased control over the higher priority data packet handling resources.

Thus, for example, in accordance with certain embodiments of the present invention, a method for forwarding packetized data in a data communications system is provided. The method includes the steps of receiving packetized data, forwarding the packetized data at a first priority unless identified as having a desired second priority. In which case, the method includes forwarding the packetized data at the

desired second priority provided the threshold traffic level associated with the second priority has not or will not be exceeded by the subscriber. Otherwise, the method includes, forwarding this packetized data at the first priority rather than the second priority.

A plurality of priority levels can be provided and higher priority data can be handled at any one of the lower priority levels. The packetized data can include, for example, data formatted in accordance with a transmission control protocol (TCP), an internet protocol (IP), a user datagram protocol(UDP), a realtime transport protocol (RTP), a realtime streaming protocol (RTSP), a reservation protocol (RSVP), and/or other like protocols. The method can also be operatively associated with a forwarding node in a network, such as, for example, a gateway, a switch, a bridge, a server, a router, or other like node.

Furthermore, in accordance with certain further embodiments of the present invention, the method further includes the step of determining the application associated with the received packetized data, and selectively forwarding the packetized data associated with a first application prior to forwarding data associated with a second application. Thus, certain applications can be provided a specific QoS. This is especially useful for applications that require time-critical packetized data.

The above stated needs and others are also met by an arrangement for forwarding packetized data in a data communications network, in accordance with certain embodiments of the present invention. The arrangement includes a source node having at least one application associated with a subscriber and configured to output packetized data. Profile data is also included in the arrangement, the profile data is associated with a particular subscriber and includes at least one threshold traffic level associated with the subscriber. The threshold traffic level defines an agreed to amount of packetized data traffic service to be provided for packetized data forwarded according to at least one priority.

The arrangement further includes a policing module, which is connected to the source node and configured to receive packetized data from the application and access the profile data, for example using a source node address or other identifier.

The policing module is further configured to forward the packetized data at a first priority, unless identified therein by the application as having a desired second priority. In which case, the policing module forwards the packetized data at the desired second priority, provided that the threshold traffic level associated with the second priority is not or would not be exceeded by the subscriber. Otherwise, the policing module forwards the packetized data at the first priority.

In accordance with certain further embodiments of the present invention, the policing module further includes a plurality of data queues and a prioritizer. The plurality of data queues includes at least a first queue configured to store the packetized data to be forwarded at the first priority, and a second queue configured to store the packetized data to be forwarded at the second priority.

The prioritizer receives the packetized data, selectively places the packetized data in at least one of the plurality of data queues, and forwards at least a portion of stored packetized data within the second queue prior to forwarding stored packetized data within the first queue.

In accordance with still further embodiments of the present invention, another arrangement is provided. This arrangement includes at least one source node, a network, at least one destination node, and a policing module.

The source node is configured to output at least two classes of packetized data, including top-priority (TP) data and best effort (BE) data.

The network is connected to the source node and configured to receive, queue and forward each of the classes of packetized data, including the TP data and the BE data.

The destination node is connected to the network and configured to receive at least one of the classes of packetized data, including at either the TP data and/or the BE data as forwarded by the network.

The policing module is configured to monitor and dynamically control queuing of at least the TP data and the BE data within the network. The policing module is configured to selectively re-queue at least a portion of the TP data with the BE data when a TP data traffic level associated with the TP data from the source node to the destination node exceeds at least one threshold traffic level. The threshold traffic level

can be a source node TP data threshold traffic level and/or a destination node TP threshold traffic level.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method and arrangements of the present invention may be had by reference to the following detailed description when taken in conjunction with the accompanying drawings wherein:

Fig. 1 is a block diagram depicting a conventional data communications system having at least one routing node configured to receive and forward packetized data, for example in the form of a datagram;

Fig. 2 is a block diagram depicting an improved routing node for use in the communications system, for example, as in Fig. 1, in accordance with certain exemplary embodiments of the present invention; and

Fig. 3 is a datagram suitable for use with an improved routing node, for example, as in Fig. 2, in accordance with certain further embodiments of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram depicting a conventional data communications system 10. Data communications system 10 is configured to allow two-way (or multidirectional) data communications between two or more communicating nodes. For simplification purposes, only two communicating nodes are depicted in Fig.1, each being labeled with respect to its function during an exemplary, one-way data communication session. Thus, as depicted in Fig. 1, there is a source 12 and a destination 28 associated with a one-way data communication of a datagram 16 from source 12 through various interconnecting resources to destination 28.

Source 12 is configured to output information in the form of data. The data output by source 12 is packetized or otherwise arranged in the form of datagram 16. For example, datagram 16 can include an IP configured data packet. Source 12 can include any device capable of outputting datagram 16. Thus, for example, source 12 can include a telecommunications terminal or other computing device configured to

convert user inputs, audio signals, still/video images, and/or the like into one or more datagrams.

Source 12 is connected to network 14 and configured to output datagram 16 through network 14 to a gateway 18. Network 14 can include any type of data network that can transport datagram 16. Thus, for example, network 14 can include a LAN, WAN, intranet, PSTN, mobile telecommunications network, and the like.

Gateway 18 provides connectivity between network 14 and network 20. Network 20 can include any type of data network that can transport datagram 16. Thus, for example, network 20 can include a LAN, WAN, intranet, the Internet, PSTN, mobile telecommunications network, and the like.

Network 20 includes a plurality of interconnected routing nodes, such as those having routers 22A-N. The routing nodes are preferably packet switched nodes configured to store and forward various datagrams 16. As such, routers 22A-N can include any communication resource/device configured to receive and selectively output datagrams 16. By way of example routers 22A-N can include routers, switches, gateways, bridges, servers, etc.

As depicted in Fig. 1, a first router 22A is connected to gateway 18 and configured to selectively receive datagram 16 and route datagram 16 to one or more connected routers 22B through 22N. In this example, datagram 16 is output by router 22A to router 22B. Router 22B is connected to a second gateway 24. Router 22B outputs datagram 16 to gateway 24.

Gateway 24 provides connectivity between network 20 and network 26. Network 26 can include any type of data network that can transport datagram 16. Thus, for example, network 26 can include a LAN, WAN, intranet, PSTN, mobile telecommunications network, and the like. As depicted in Fig. 1, destination node 28 is connected to network 26 and configured to receive datagram 16 therefrom.

Destination node 28 is configured to process the information contained within datagram 16. As such, destination node 28 can include any device capable of outputting datagram 16. Thus, for example, destination node 28 can include a telecommunications terminal or other computing device configured to convert datagram 16 into corresponding user outputs, audio signals, still/video images, etc.

A policing module 38 is depicted in Fig. 2, in accordance with certain embodiments of the present invention. Policing module 38, which may be incorporated into any interface, switching or routing node within a communications system or network, is configured to receive, prioritize and output datagrams. Thus, for example, policing module 38 can be included in any one of the gateways 18/24, and/or routers 22A-N. policing module 38 can also be employed elsewhere within networks 14 and/or 26, as appropriate. Preferably, policing module 38 is included in each routing node.

Policing module 38 is configured to receive a datagram 16' and to selectively output datagram 16'. As depicted in the exemplary embodiment of Fig. 2, policing module 38 includes a prioritizer 30, a plurality of data queues 32, and user profiles 34. Alternatively, all or part of user profiles 34 can be external to policing module 38, and may be centrally located or otherwise provided for use by a plurality of similarly configured nodes. User profiles 34 are, in certain configurations, simply data associated with subscribers that can be stored/retrieved, for example, in/from a database connected to network 20 or otherwise connected to a routing node therein.

In the examples, below, it is assumed that datagram 16' can be labeled as either a top priority (TP) datagram, or a best effort (BE) datagram. For example, for IP the ToS byte can be modified, or another portion of the protocol's header can be used. Continuing with the above example, let us assume that a TP datagram has a higher priority than a BE datagram, with regard to routing decisions within the network and the desired/resulting QoS.

Thus, for example, realtime or time-critical data, such as audio and video data, is preferably transported using TP datagrams rather than BE datagrams. Although this example uses only two different priorities, it should be clear that more than two priorities can be defined.

User profiles 34 provide information about the various users or subscribers that can send/receive datagram 16'. By way of example, in accordance with certain preferred embodiments of the present invention, user profiles 34 include information in the form of data defining the subscriber's capability to send/receive datagrams

having different priorities and (optionally) the various applications that may be used by the subscriber.

Thus, at a minimum, user profiles 34 includes at least one identifier defining a TP threshold level 36 associated with an agreed to level of service to be provided by the communications service provider for a given subscriber. If multiple priority levels are to be provided, then user profiles 34 can include a plurality of corresponding threshold levels.

As described in more detail below, threshold level 36 is used to determine if a subscriber (either sender or receiver) is operating within their agreed to service. Should a subscriber exceed the agreed to service, for example, by attempting to send/receive a number of TP datagrams (over a period of time) greater than the TP threshold level 36, then policing module 38 will dynamically alter the handling of such TP datagrams. Furthermore, policing module 36 can report this status and other monitored information to other network resources for further processing. This provides additional control over the network and its subscribers.

Prioritizer 30 is configured to receive datagram 16′ and at least threshold level 36 from user profiles 34. Prioritizer 30 determines the priority of datagram 16′ (e.g., TP, or BE) by examining a priority identifier 40 within datagram 16′ (see, Fig. 3). Prioritizer 30 is further configured to monitor the status of data queues 32A-K and to determine an appropriate data queue for the received datagram 16′. Each of the data queues 32A-K is associated with at least one datagram priority level and is preferably configured as a first-in-first-out (FIFO) configuration and data queues serving higher priority datagrams are emptied first.

Thus, in the example above, data queue 32A can be associated with TP datagrams and data queue 32B can be associated with BE datagrams.

In this example, therefore, there are four possible scenarios that need to be handled by policing module 38:

1.) If a BE datagram 16′ (i.e., a lower priority datagram) is received and the BE data queue 32B (i.e., a lower priority queue) is not overflowing, then prioritizer 30 places the BE datagram 16′ in data queue 32B;

2.) If a BE datagram 16′ is received and the BE data queue 32B is overflowing, then prioritizer 30 drops (i.e., does not forward) the received BE datagram 16′;

3.) If a TP datagram 16′ (i.e., a higher priority datagram) is received and the TP data queue 32A (i.e., higher priority data queue) is not overflowing, then prioritizer 30 compares the amount of TP traffic sent/received by the subscriber(s) during a preceding period of time with the TP threshold level 36, such that,

a.) if the TP threshold level 36 has not been exceeded by the subscriber(s), then the received TP datagram 16′ is placed in the TP data queue 32A, else

b.) if the TP threshold level 36 has been (or would be) exceeded by the subscriber(s), then the received TP datagram 16′ is treated as having a lower priory, in this example, it is treated according to scenarios 1.) or 2.), above.

Thus, when the higher priority's threshold level 36 is exceeded (or would be exceeded), the priority label of the datagram 16′ is essentially ignored and the datagram 16′ is temporarily re-prioritized to a lower priority. If there are more than two priority levels, then the re-prioritization (e.g., re-queuing) can be decremented or otherwise configured accordingly to allow for the next highest available priority data queue to be used.

In accordance with still further embodiments of the present invention, policing module 38 is configured to allow certain subscribers to exceed threshold level 36, provided that resources are available to handle such additional higher priority traffic. Thus, for example, user profile 34 can further specify that the subscriber can exceed threshold 36 at times. Additionally, priority identifier 40 or other data within the datagram can be used by the application to identify that the datagram should not be re-prioritized, if possible. Subscribers that exceed their agreed to threshold 36 can be charged accordingly for this added service/capability.

Fig. 3 graphically depicts a datagram 16′, in accordance with certain embodiments of the present invention. Datagram 16′ includes at least a priority identifier 40 that identifies the desired priority level for the related data therein. Thus, for example, in accordance with certain embodiments of the present invention,

datagram 16′ is an IP datagram and priority identifier 40 is included in the ToS byte. Realtime data 44 can also be included in datagram 16′. Realtime data includes any time-critical data, such as, for example, audio, video, or other image data.

In accordance with still further embodiments of the present invention, an application identifier 42 can also be provided in datagram 16′. Application identifier 42 identifies the type of application being used at the source/destination nodes. Thus, for example, application identifier 42 can identify that datagram 16′ is associated with an audio signal, a video signal, etc., and/or that the datagram is associated with a critical application, non-critical application, etc. In this manner, prioritizer 30 can gain additional information about the ongoing communication and can further alter the handling of datagram 16′ accordingly. Application identifier 42 can be combined with or separate from priority identifier 40.

By way of example, prioritizer 30 can use the information relayed in application identifier 42 to further determine how to best handle the received datagram 16′. Thus, a VoIP application's TP datagram 16′ may be given priority over a non-VoIP application's TP datagram 16′ within the TP data queue 32A, thereby causing non-VoIP application TP datagrams to be re-prioritized (or re-queued) should the TP data queue 32A become full. Further enhancements can include providing additional data queues 32 for use with different applications, wherein each additional data queue 32 has at least one corresponding priority level.

In the manner, prioritizer 30 can be fine-tuned to increase the QoS for selected priorities/applications and/or maximize system utilization. By selectively, dynamically and momentarily re-prioritizing or re-queuing the datagram, policing module 38 significantly reduces the potential for dropping higher priority datagrams.

By including policing module 38 at a plurality of interconnected nodes in a data communications system/network, the overall control of the system/network can be increased. As such, the communications service providers can provide additional incentives to subscribers to either select certain services, and/or to avoid exceeding the agreed to services.

Policing module 30 can be embodied in hardware or software, and where applicable can be standalone or distributed or otherwise arranged among various nodes as required to further enhance the additional features supported.

Although some preferred embodiments of the methods and arrangements of the present invention have been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it will be understood that the invention is not limited to the embodiment disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

WHAT IS CLAIMED IS:

1. A method for forwarding packetized data in a data communications system, the method comprising the steps of:

receiving packetized data from at least a first application and a second application associated with a subscriber;

providing at least one threshold traffic level associated with said subscriber, said threshold traffic level defining an agreed to amount of packetized data traffic service to be provided for packetized data forwarded according to at least one priority;

determining an application type of said first application and said second application associated with said received packetized data;

forwarding the packetized data at a first priority unless identified therein by said first and said second application as having a desired second priority;

determining whether forwarding said packetized data associated with said first application and said second application exceeds said threshold traffic level for said second priority; and

if so, forwarding at said desired second priority said packetized data associated with said first application prior to forwarding said packetized data associated with said second application based upon a comparison of said application type of said first application and said second application.

2. The method as recited in Claim 1, wherein said first priority represents a lower level of quality of service (QoS)than said second priority, and said step of forwarding said packetized data at said first priority further includes using a best effort service that does not guarantee timely delivery of said packetized data.

3. The method as recited in Claim 1, wherein said second priority represents a higher level of quality of service (QoS) than does said first priority, and said method further comprises the steps of:

storing said packetized data to be forwarded at said first priority in a first

queue;

storing said packetized data to be forwarded at said second priority in a second queue; and

forwarding at least a portion of stored packetized data within said second queue prior to forwarding stored packetized data within said first queue.

4. The method as recited in Claim 1, wherein said packetized data includes information associated with at least one protocol selected from a set of protocols including a transmission control protocol (TCP), an Internet protocol (IP), a user datagram protocol(UDP), a realtime transport protocol (RTP), a realtime streaming protocol (RTSP), and a reservation protocol (RSVP).

5. The method as recited in Claim 1, wherein said method is operatively associated with at least one forwarding node selected from a set of forwarding nodes including a gateway, a switch, a bridge, a server, and a router.

6. The method as recited in Claim 1, further comprising the step of, for certain subscribers, forwarding at said desired second priority said packetized data associated with said first application and said second application when said threshold traffic level associated with said second priority is exceeded by said subscriber, so long as network resources are available and profile information associated with said certain subscribers authorizes said certain subscribers to exceed said threshold traffic level.

7. An arrangement for forwarding packetized data in a data communications network, the arrangement comprising:

a source node having at least one application that is associated with a subscriber and configured to output packetized data;

profile data associated with said subscriber, said profile data including at least one threshold traffic level associated with said subscriber, said threshold traffic level defining an agreed to amount of packetized data traffic service to be provided for

packetized data forwarded according to at least one priority;

a policing module connected to said source node and configured to receive packetized data from said application and access said profile data, said policing module being further configured to:

forward said packetized data at a first priority unless identified therein by said application as having a desired second priority,

forward said packetized data at said desired second priority, as identified therein by said application, provided said threshold traffic level associated with said second priority is not exceeded by said subscriber, and

forward said packetized data at said desired second priority, as identified therein by said application, when said threshold traffic level associated with said second priority is exceeded by said subscriber, provided network resources are available and said profile data associated with said subscriber authorizes said threshold traffic level to be exceeded by said subscriber, otherwise forward said packetized data at said first priority.

8. The arrangement as recited in Claim 7, wherein said first priority represents a lower level of quality of service (QoS)than said second priority, and said policing module forwards said packetized data at said first priority using a best effort service that does not guarantee timely delivery of said packetized data.

9. The arrangement as recited in Claim 7, wherein said second priority represents a higher level of quality of service (QoS) than does said first priority, and said policing module further includes:

a plurality of data queues including at least a first queue configured to store said packetized data to be forwarded at said first priority, and a second queue configured to store said packetized data to be forwarded at said second priority; and

a prioritizer connected to the plurality of data queue and configured to receive said packetized data, selectively place said packetized data in at least one of said plurality of data queues, and forward at least a portion of stored packetized data within said second queue prior to forwarding stored packetized data within said first queue.

10. The arrangement as recited in Claim 7, wherein said packetized data includes information associated with at least one protocol selected from a set of protocols including a transmission control protocol (TCP), an Internet protocol (IP), a user datagram protocol(UDP), a realtime transport protocol (RTP), a realtime streaming protocol (RTSP), and a reservation protocol (RSVP).

11. The arrangement as recited in Claim 7, wherein said policing module is further configured to determine an application type of said application associated with said received packetized data, and selectively forward said packetized data associated with a first application prior to forwarding data associated with a second application based upon said application type and whether said threshold traffic level associated with said second priority is exceeded by said subscriber.

12. The arrangement as recited in Claim 7, wherein said policing module is operatively coupled to at least one forwarding node selected from a set of forwarding nodes including a gateway, a switch, a bridge, a server, and a router.

13. An arrangement comprising:

at least one source node configured to output at least two classes of packetized data, including top-priority (TP) data and best effort (BE) data;

a network connected said source node and configured to receive, queue and forward each of said at least two classes of packetized data, including said TP data and said BE data;

at least one destination node connected to said network and configured to receive at least one of said at least two classes of packetized data, including at least one class of packetized data selected from among said TP data and said BE data as forwarded by said network; and

a policing module within said network and configured to monitor and dynamically control queuing of at least said TP data and said BE data within said

network, said policing module being further configured to selectively re-queue at least a portion of said TP data with said BE data when a TP data traffic level associated with said TP data from said source node to said destination node exceeds at least one threshold traffic level selected from among a source node TP data threshold traffic level and a destination node TP threshold traffic level.

14. The arrangement as recited in Claim 13, wherein said policing module further includes:

at least one TP data queue configured to receive and output said TP data;

at least one BE data queue configured to receive and output at least said BE data and said selectively re-queued TP data; and

a prioritizer connected to said TP data queue and said BE data queue and configured to monitor said TP data traffic level in said TP data queue and selectively direct TP data to said BE data queue if said TP data traffic level exceeds said at least one threshold traffic level.

15. The arrangement as recited in Claim 13, wherein said at least one TP data queue is further configured to receive and output TP data from a plurality of source node applications and said prioritizer is further configured to differentiate between source node applications and to selectively direct TP data to said TP data queue and said BE data queue based on said source node application, such that certain source node applications are provided a higher priority than other source node applications.

16. The arrangement as recited in Claim 13, wherein said BE data is provided a lower level quality of service (QoS) than said TP data, and said policing module is configured to forward said BE data and said re-queued TP data using a best effort service that does not guarantee timely delivery of said BE data and said re-queued TP data.

17. The arrangement as recited in Claim 13, wherein said TP data is

provided a higher level quality of service (QoS) than said BE data and said re-queued TP data.

18. The arrangement as recited in Claim 13, wherein said packetized data includes information associated with at least one protocol selected from a set of protocols including a transmission control protocol (TCP), an Internet protocol (IP), a user datagram protocol(UDP), a realtime transport protocol (RTP), a realtime streaming protocol (RTSP), and a reservation protocol (RSVP).

19. The arrangement as recited in Claim 13, wherein said policing module is operatively coupled to at least one forwarding node selected from a set of forwarding nodes including a gateway, a switch, a bridge, a server, and a router.

20. The arrangement as recited in Claim 13, wherein said policing module is further configured to selectively allow at least a portion of said TP data to continue to be queued as TP data even though said TP data traffic level associated with said TP data from said source node to said destination node exceeds said threshold traffic level selected from among said source node TP data threshold traffic level and said destination node TP threshold traffic level, provided that suitable network resources are available and said subscriber is authorized to temporarily exceed said threshold traffic level, otherwise, re-queue said portion of said TP data with said BE data.

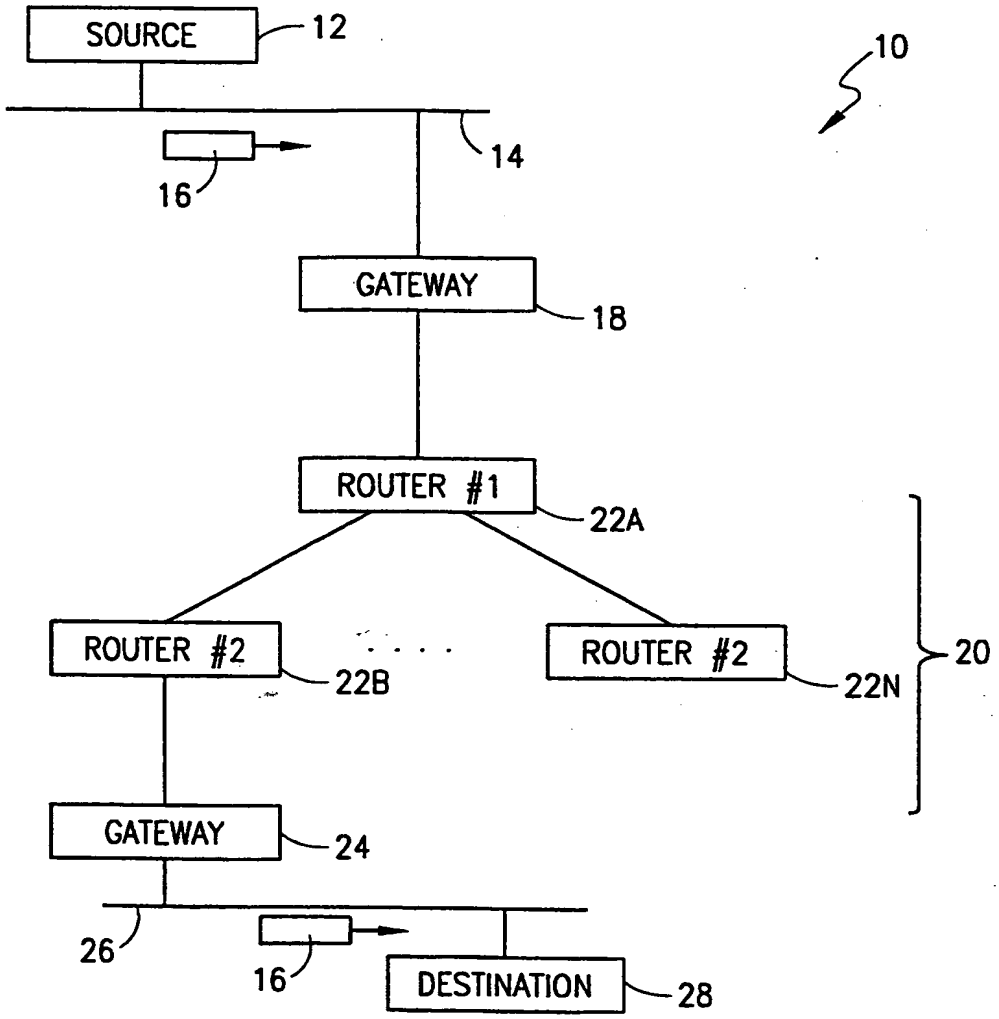


FIG. 1
(PRIOR ART)

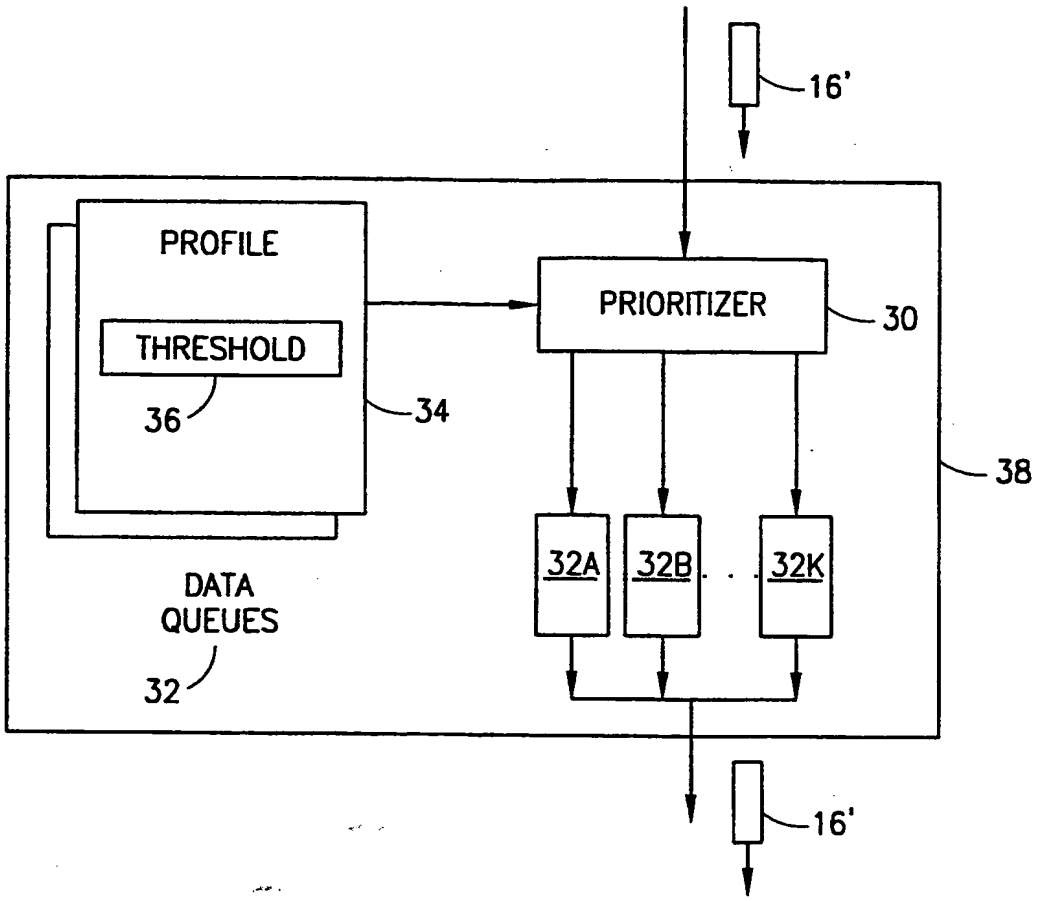

16'
PROFILE
THRESHOLD
36
34
PRIORITIZER
30
38
32A
32B
32K
DATA
QUEUES
32
16'

FIG. 2

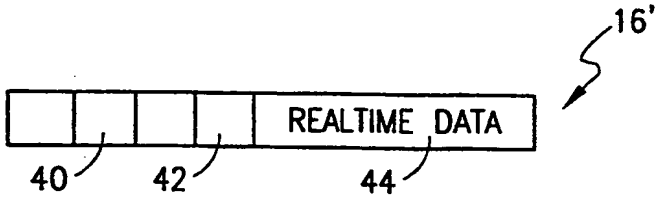

16'
REALTIME DATA
40
42
44

FIG. 3

INTERNATIONAL SEARCH REPORT

In. ational Application No
PCT/SE 00/00503

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/56 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 581 545 A (MORITOMO HARUO) 3 December 1996 (1996-12-03) column 6, line 31 -column 7, line 2; figure 8	7,8, 12-14, 16,17, 19,20
Y		9,10,15, 18
A		1,2,5,6

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 July 2000	25/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ströbeck, A

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE 00/00503

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	O'NEILL A ET AL: "AN OVERVIEW OF INTERNET PROTOCOLS" BT TECHNOLOGY JOURNAL, vol. 16, no. 1, 1 January 1998 (1998-01-01), pages 126-139, XP000736934 ISSN: 0265-0193 page 133, left-hand column, line 17 -right-hand column, line 4	9
Y	ALMESBERGER W ET AL: "SRP: A SCALABLE RESOURCE RESERVATION PROTOCOL FOR THE INTERNET" COMPUTER COMMUNICATIONS, vol. 21, no. 4, 15 September 1998 (1998-09-15), pages 1200-1211, XP000667615 ISSN: 0140-3664 page 1202, left-hand column, line 4 -right-hand column, line 24 page 1206, right-hand column, line 26 -page 1207, left-hand column, line 7	10,18
Y	WO 97 41674 A (3COM CORP) 6 November 1997 (1997-11-06) page 8, line 33 -page 10, line 32	15
A	EP 0 658 999 A (NEC CORPORATION) 21 June 1995 (1995-06-21) page 2, line 36 - line 49 page 3, line 47 - line 57	1,2,5,6

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ational Application No
PCT/SE 00/00503

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5581545 A	03-12-1996	JP 7264189 A	13-10-1995
		US 5737315 A	07-04-1998
WO 9741674 A	06-11-1997	AU 2820697 A	19-11-1997
EP 0658999 A	21-06-1995	US 5530695 A	25-06-1996
		CA 2118471 A	16-06-1995
		JP 7170274 A	04-07-1995